JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko

Asia: VNS 4/2020 vp

Professori, ST Martti Lehto

11.12.2020

Yhteiskunnan digitalisaatio

Digitalisaatio hyödyttää kansalaisia, yrityksiä ja julkisia toimijoita



Kyber- ja informaatio-operaatioilla voidaan lamauttaa yhteiskunnan kriittistä infrastruktuuria ja elintärkeitä toimintoja

Kehityksen ajureita ovat massadata, pilviteknologia, autonomia ja tekoäly



eBank eTravel eAccommodation eTraffic

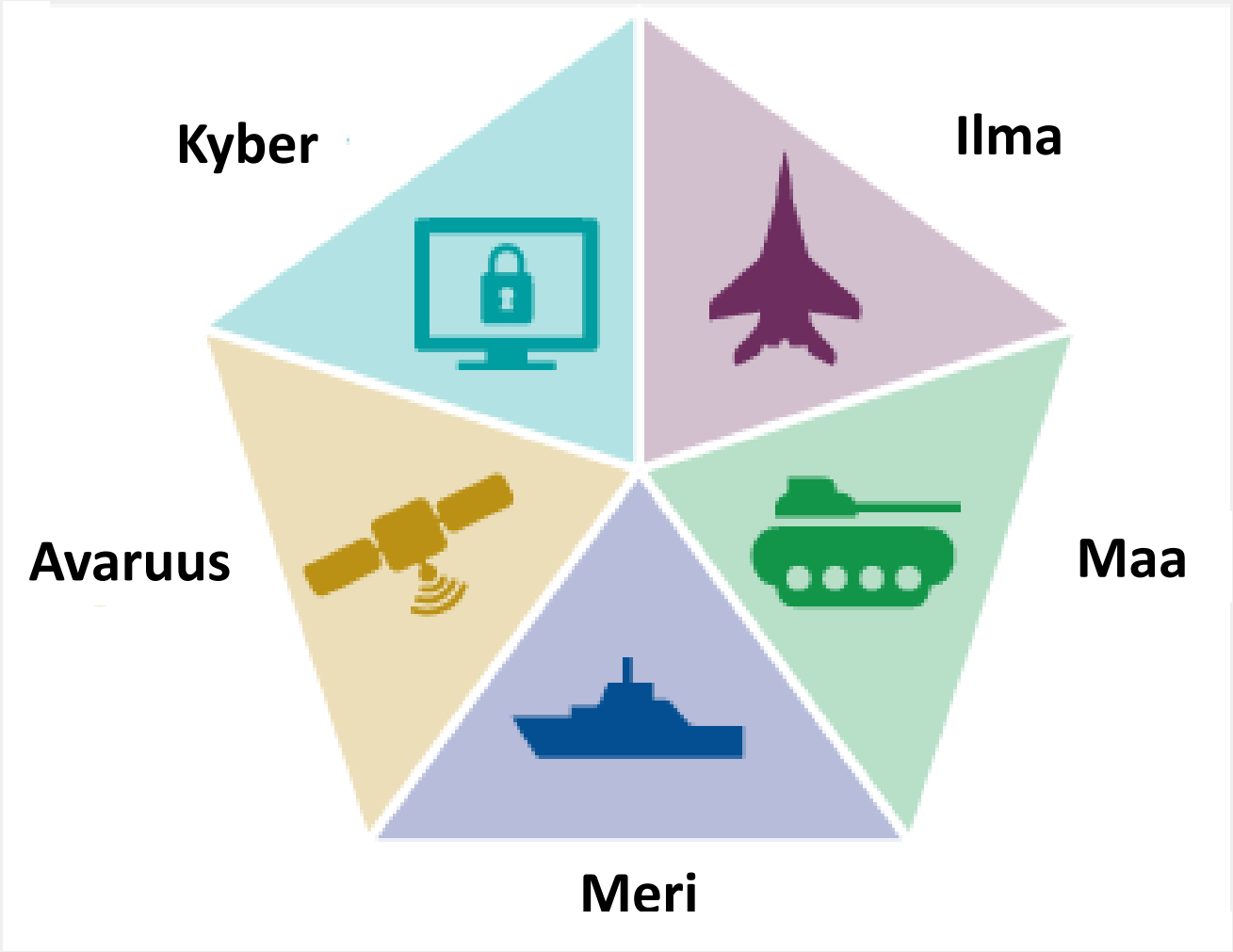
eBusiness eEnt eMedia eSharing Economy

eHealth eAssistant ePartner eAdministration

Kansallinen kybertila

Aluevalvontalaki (18.8.2000/755) kuvaa Suomen valtakunnan aluetta määrittelemällä maa- ja merirajoja ja niiden yläpuolista ilmatilaa.

AKV/AKT

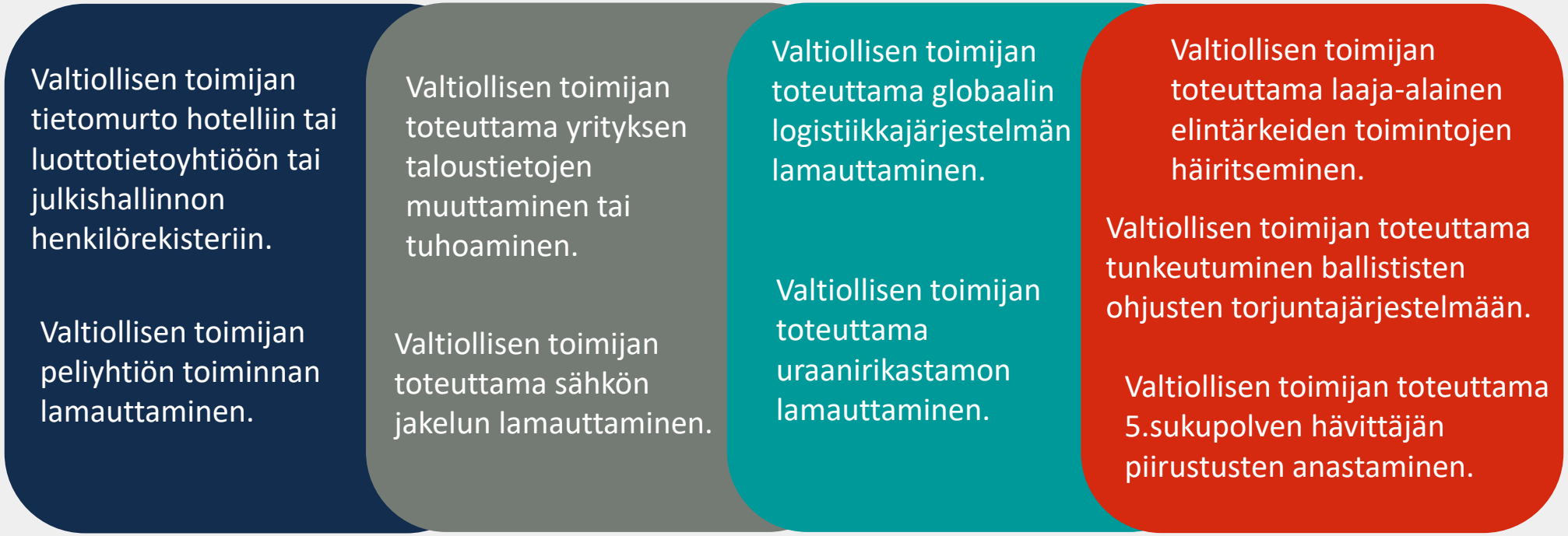


Kansallinen kybertila tulisi määritellä, jotta voitaisiin toteuttaa Suomen kybertilan koskemattomuuden valvonta ja torjunta.

Kansallinen suvereniteetti kybertilassa-

5,20 miljardia (67 %) matkapuhelimen käyttäjää.	4,66 miljardia (59,7 %). Internetin käyttäjää.	4,14 miljardia (53 %) sosiaalisen median käyttäjää.

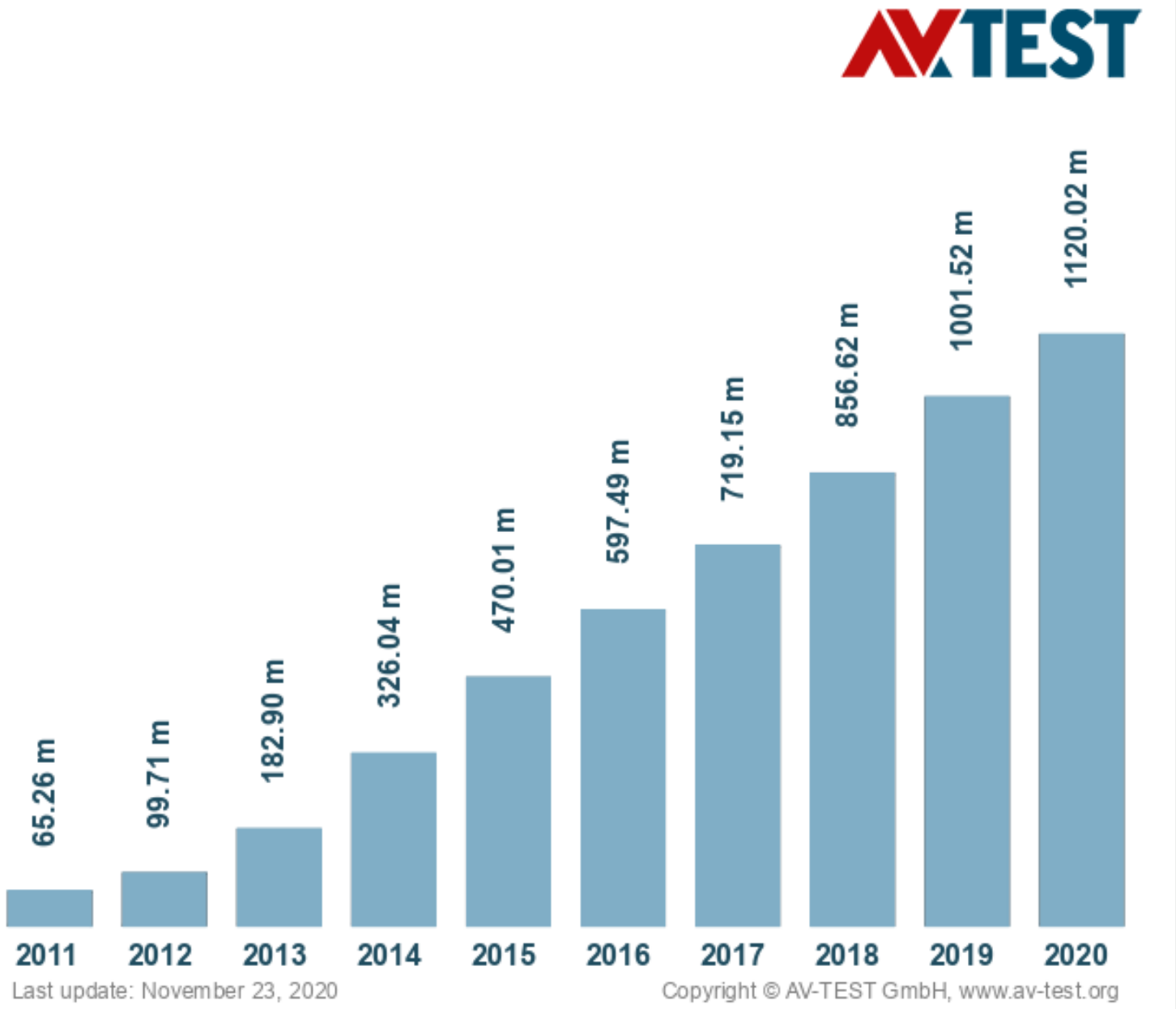
Sota ja rauha kybertilassa



Operaatioita sodan kynnyksen alapuolella

Kyber-maailma 2025?

Yhdysvallat	Kiina	Venäjä
Google	Baidu Tieba	Yandex
Whatsapp	WeChat	Telegram
YouTube	Youku Tudou	RuTube
Amazon	AliBaba	Avito
Instagram	Nice, Meipai	Moi Mir
Twitter	Weibo	Futubra
Uber	DidiKuaidi	Yandex-Uber
Expedia	C-trip	Aviasales
Apple Pay	Alipay	Payonline
Wikipedia	Chinese Encyclopedia	Big Russian Encyclopedia
Facebook	Renren	Vkontakte, Odnoklassniki
Gmail/Hotmail/Yahoo	QQMail/AliMail	Mail.ru
Internet	China Net	RuNet



Haittaohjelma-tuotanto

350 000 uutta haittaohjelmaa joka päivä

Source: https://www.av-test.org/en/statistics/malware/

Kriittinen infrastruktuuri kybersabotaasin kohteena



Chemical





Dams





Financial Services





Information Technology







Commercial Facilities





Defense Industrial Base





Food & Agriculture





Nuclear Reactors, Materials & Waste

e.g., power plants, power nuclear rea research





Communications





Emergency Services





Government Facilities

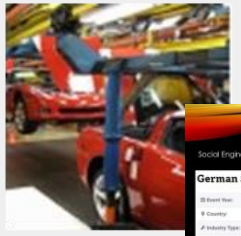




Transportation Systems

e.g., aviation, h maritime, mass pipeline, freigh shipping





Critical Manufacturing





Energy





Healthcare & Public Health





Water & Wastewater Systems

e.g., public drinking w systems, treatment s



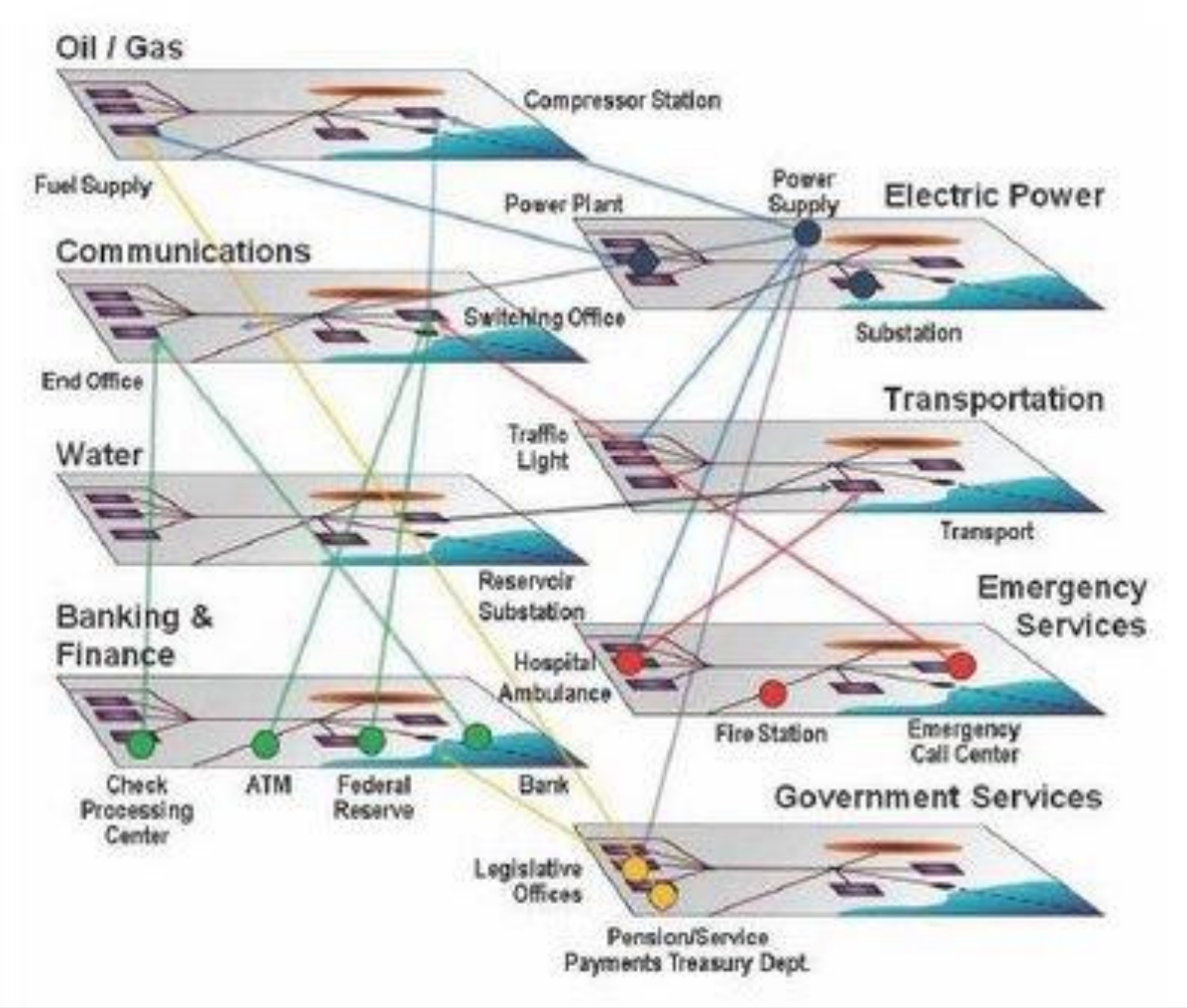
Kriittinen infrastruktuuri

Poliittinen ulottuvuus: Kansallinen turvaamisen intressi, kansallinen lainsäädäntö, kansainvälinen yhteistyö.

Taloudellinen ulottuvuus: Yksityiset ja julkiset toimijat, turvaamiskustannukset.

Teknologinen ulottuvuus: tekniset järjestelmät ja ratkaisut.

Vahva kansallisen kriittisen infrastruktuurin kyberturvallisuusohjelma



Informaatiovaikuttamisen torjunnan kehittäminen

Kenen vastuulla on yhteiskuntaan kohdistuvan informaatiovaikuttamisen torjunnan toteuttaminen?

Kuka vastaa Suomen henkisen tilan hallinnasta?

Kuinka hoidetaan normaaliaikoina esiintyvien informaatio-operaatioiden torjunta.



Informaatiovaikuttamisen torjunnan kehittäminen

EU: ”On hyvin tärkeää, että hybridiuhkiin kyetään vastaamaan pätevällä **strategisen viestinnän** strategialla.”



Kansallinen informaatiovaikuttamisen torjunnan/informaatiopuolustuksen ohjelma

Kyberturvallisuuden strategisen johtamisen haaste 1

Keskeisin haaste kansallisen kyberturvallisuuden toteuttamisessa on toiminnan hajautuminen laajalle eri toimijoiden vastuulle.

Kyberturvallisuusasiat ja informaatiovaikuttaminen näyttäytyvät nykyisin arkisina niin kriittisen infrastruktuurin ja yrityksien kuin kansalaisten piirissä.

Kyberturvallisuuden strateginen johtaminen on tätä arjen toimintaa laajempi kokonaisuus käsittäen myös kansallisen turvallisuuden ja suvereniteetin kybertilassa.



Kyberturvallisuuden strategisen johtamisen haaste 2

Kyberturvallisuuden strategisen johtaminen on valtion kyvykkyyksien ja elintärkeiden toimintojen turvaamista sekä normaaliaikoina että poikkeusoloissa.

Puolustusvoimat

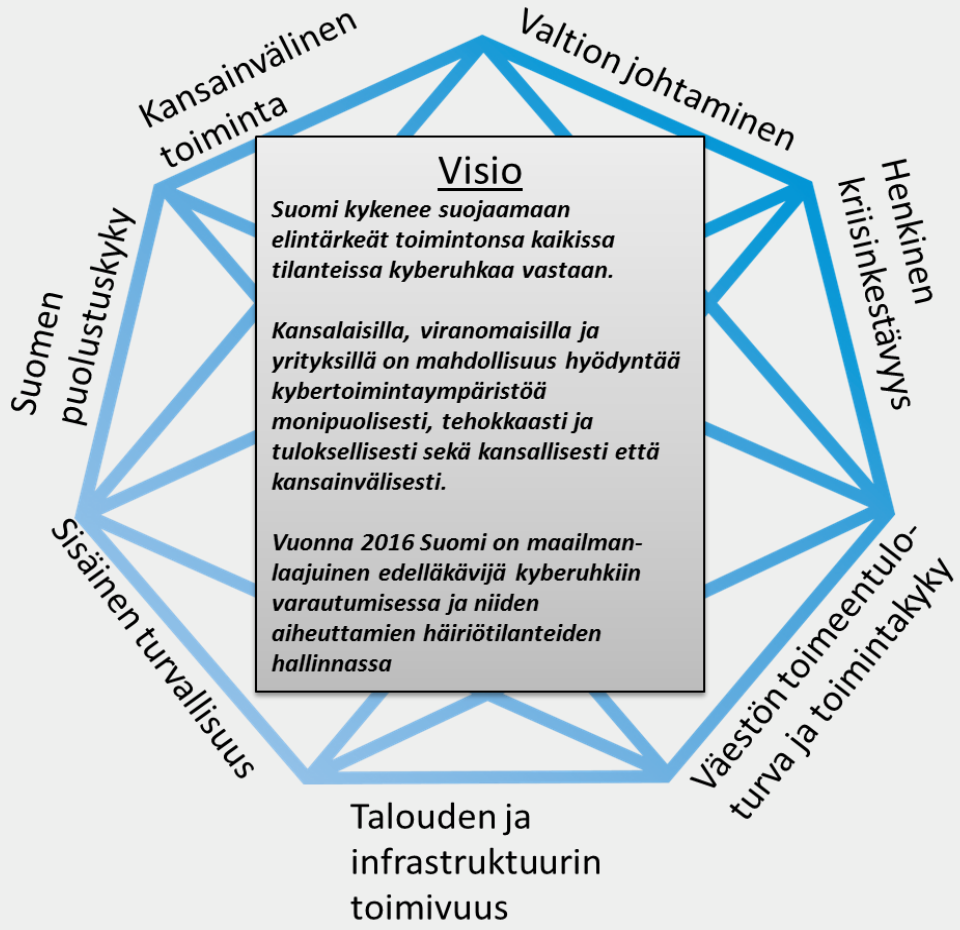
SUPO

Kyberturvallisuuskeskus/LVM

Huoltovarmuuskeskus



Suomen kyberturvallisuuden tila 2020



Suomen suhteellinen asema hyvänä kyberturvallisuusmaana on heikentynyt vuodesta 2012 lähtien.

Erilaisilla kansainvälisillä indekseillä mitataan maiden kyberturvallisuuskyvykkyyttä ja näissä arvioinneissa maamme asema suhteessa muihin on alentunut.

Global Cybersecurity Index

Suomi
- Index 0.618
- EUR: 5
- Global: 8

GSI 2014



GSI 2017

Suomi
- Index 0.741
- EUR: 6
- Global: 16

GSI 2018

Suomi
- Index 0.856
- EUR: 10
- Global: 19

National Cyber Security Index

Suomi
- Index 79,22
- Rank: 5
- DDL: 82,26
- Ero: -3,04

NCSI 2018



NCSI 2020

Suomi
- Index 81,82
- Rank: 10
- DDL: 82,26
- Ero: -0,44

Kyberturvallisuuden strateginen johtaminen

Koska kyber on kaikkialla, tarvitaan kansallinen kyberturvallisuuden strateginen johtamismalli, joka tukisi kyberturvallisuuden kokonaisvaltaista varautumista kehittämistä ja laajamittaisten häiriötilanteiden hallintaa.

Asejärjestelmien autonomia

Selonteon mukaan ”Täysin autonomisia, kokonaan ihmisen kontrollin ulottumattomissa olevia asejärjestelmiä ei pidä kehittää jatkossakaan.”

Kuka painaa liipaisinta?

Mikä on ihmisen kontrolli liipaisimen painamisen jälkeen.

Voiko maalin valintaa ulkoistaa?

Autonomisia asejärjestelmiä

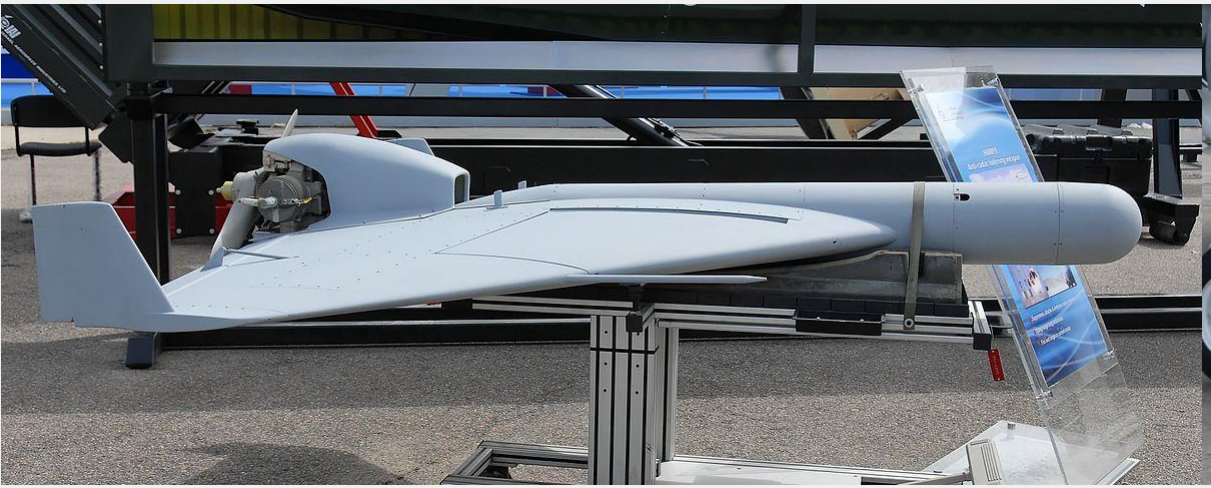
The **Phalanx** autonominen tutkaohjattu tykki, joka on tarkoitettu torjumaan meri- ja maamaaliohjuksia



Iron Dome: täysin autonominen ohjusten ja rakettien torjuntajärjestelmä.



Harpy vs. HARM



IAI, Harpy



Raytheon, AGM-88 HARM

	Ase	Maali	Etsintäaika	Toimintaetäisyys	Autonomia-aste
HARM	Hakeutuva ohjus	Tutka	Noin 4,5 minuuttia	90+ km	Semiautonominen ase
Harpy	Vaaniva ase	Tutka	2,5 tuntia	500 km	Täysin autonominen ase

Russia is building an AI-powered missile that can think for itself



FEATURES | SECURITY | CHINA

Is China Really Building Missiles With Artificial Intelligence?

There are real limits on the amount of AI acceptable to navy commanders.

By Abhijit Singh
September 21, 2016



Military missiles are presented during the military parade marking the 70th anniversary of the end of World War II, in Beijing, China (September 3, 2015.)

Image Credit: REUTERS/Rolex Dela Pena/Pool

With rising security challenges in the global commons, there is growing interest in the subject of "intelligent" weapons systems. This is especially so in the maritime realm, where recent studies have shown that precision-guided weaponry and networked systems are likely to play an increasingly important role. Even while accepting autonomous systems as the future of maritime warfare, however, many find the subject of "intelligent weapon systems" to be deeply contentious.

Today's most advanced weapons are already capable of "making decisions" using built-in smart sensors and tools.

Kiitos

www.jyu.fi/it

